

What is claimed is:

- 1           1. A method, comprising:
  - 2               based on policy rules, creating an access control
  - 3               list adapted to configure a network device; and
  - 4               using the access control list to generate access
  - 5               filters.
- 1           2. The method of claim 1 further comprising expanding
  - 2               the policy rules into value groups that represent
  - 3               conditions associated with the policy rules.
- 1           3. The method of claim 2 further comprising excluding
  - 2               conditions that would otherwise be implied by the
  - 3               rules.
- 1           4. The method of claim 3 further comprising resolving
  - 2               inconsistent conditions that result from expanding
  - 3               the policy rules and excluding the policy rule
  - 4               conditions.
- 1           5. The method of claim 1 further comprising creating at
  - 2               least one array of included or excluded conditions
  - 3               from the policy rules.
- 1           6. The method of claim 5 wherein generating the access
  - 2               filters further comprises:
    - 3                   adding filters adapted to control access of a device
    - 4                   to another component in the network.
- 1           7. The method of claim 6 further comprising generating
  - 2               deny filters by combining the at least one array of
  - 3               excluded conditions and the at least one array of
  - 4               included conditions.
- 1           8. The method of claim 6 further comprising generating
  - 2               permit filters by combining the at least one of the

arrays of the included conditions with the remaining  
arrays of included conditions.

9. A computer network, comprising:

a first device adapted to disseminate policy rules  
in the network; and

a second device adapted to receive the policy rules  
disseminated on the network by the first device and  
adapted to:

based on policy rules, create an access  
control list adapted to configure the at  
least one device from the filters;

and to use the access control list to  
generate access filters from the  
translated policies.

10. The system of claim 9 wherein the second device  
further comprises a permit filter.

11. The system of claim 10 further comprising a  
plurality of data-storage devices adapted to permit  
access to the second device.

12. The system of claim 9 wherein the second device  
further comprises a deny filter.

13. The system of claim 12 further comprising a  
plurality of data-storage devices adapted to deny  
access to the second device.

14. An article comprising a computer-readable medium  
which stores computer executable instructions for  
managing policy rules on a network, the instructions  
causing a computer to:

5 based on policy rules, create an access control  
6 list adapted to configure the devices from the simplified  
7 rules; and

8 use the access control list to generate access  
9 filters.

1 15. The article of claim 14 further comprising  
2 instructions to expand the policy rules into value  
3 groups, wherein value groups represent conditions  
4 associated with the policy rules.

1 16. The article of claim 15 wherein the instructions to  
2 translate the policy rules further includes  
3 instructions to exclude conditions that would  
4 otherwise be implied by the policy rules.

1 17. The article of claim 16 wherein the instructions to  
2 translate the policy rules further includes  
3 instructions to resolve inconsistent conditions that  
4 result from expanding the policy rules and excluding  
5 the policy rule conditions.

1 18. A network device, comprising:

2 a configurable management process located on the device

3 having instructions to:

4 receive the policy rules in a network device;

5 translate the policy rules to a set of  
6 simplified rules;

7 create an access control list adapted to  
8 configure the devices from the simplified rules; and

9 use the access control list to generate access  
10 filters.

1 19. The device of claim 18 further comprising a  
2 connection to an external network.

1 20. The device of claim 19 wherein the external network  
2 is a local area network.

1 21. The device of claim 19 wherein the external network  
2 is the Internet.

1 22. A method of managing access by a device on a network  
2 to another component on the network, comprising:  
3 providing policy rules that determine the access of  
4 the device to the component.

1 23. The method of claim 22 wherein the policy rules  
2 comprise:

3 an access control list including the conditions that  
4 allow the device to access the component; and  
5 filters for implementing the access.

1 24. The method of claim 22 wherein the access control  
2 list comprises include and exclude arrays that are combined to  
3 generate the filters.